

The PROLiNK logo is displayed in white, bold, sans-serif capital letters within a blue rectangular box. A registered trademark symbol (®) is located at the top right of the word.

PROLiNK®

Challenge The Limit

USER MANUAL

PROLiNK® Wireless-N Portable Router WNR1004

Revision 1.0 (Apr'09)

Copyright

The contents of this publication may not be reproduced in any part or as a whole, stored, transcribed in an information retrieval system, translated into any language, or transmitted in any form or by any means, mechanical, magnetic, electronic, optical, photocopying, manual, or otherwise, without the prior written permission.

Trademarks

All products, company, brand names are trademarks or registered trademarks of their respective companies. They are used for identification purpose only. Specifications are subject to be changed without prior notice.

FCC Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against radio interference in a commercial environment. This equipment can generate, use and radiate radio frequency energy and, if not installed and used in accordance with the instructions in this manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his own expense, will be required to take whatever measures are necessary to correct the interference.

CE Declaration of Conformity

This equipment complies with the requirements relating to electromagnetic compatibility, EN 55022/A1 Class B.

Table of Contents

CHAPTER 1: INTRODUCTION	1
1.1 Features	1
1.2 Physical Details	2
CHAPTER 2: ABOUT OPERATION MODES	3
2.1 Operation Modes	3
2.2 Access Point Mode.....	3
2.3 Gateway Mode.....	4
2.4 Client Mode	4
CHAPTER 3: CONFIGURATION.....	5
3.1 Hardware Connection.....	5
3.2 Login	5
3.3 Wizard (Gateway Mode)	8
3.4 Internet Settings.....	13
3.5 Wireless Settings.....	21
3.6 Firewall	41
3.7 Administrators	45
CHAPTER 4: PC CONFIGURATION	49
4.1 Overview.....	49
4.2 Windows Clients.....	49
4.3 Macintosh Clients	53
4.4 Linux Clients.....	54
4.5 Other Unix Systems	54
4.6 Wireless Station Configuration	55
APPENDIX A: TROUBLESHOOTING	56
A.1 Overview.....	56
A.2 General Problems	56
A.3 Internet Access	56
A.4 Wireless Access.....	57
APPENDIX B: ABOUT WIRELESS LANS.....	58
B.1 BBS.....	58
B.2 Channels.....	58
B.3 Security	58
APPENDIX C: TECHNICAL SUPPORT	61
C.1 Register Online for Free Warranty	61

Chapter 1: Introduction

This is a compact/travel size IEEE802.11b/g/n router with 2 fast Ethernet ports, which provides a powerful high-speed wireless connection for compatible wireless-enabled devices into the network with the freedom to roam. With web-based UI, this Access Point is easy to be setup and maintained. All functions can be configured within the easy and friendly user interface via web browser. Via the fast wireless network speed up to 150 Mbps, you can be very comfortable to have experience of high speed web surfing, files downloading, online game playing, and video conference session and streaming high quality multimedia materials. The Wireless Portable Router provides WPA/WPA2, 64/128 bit WEP encryption and IEEE802.1x which ensures a high level of security to protect users' data and privacy when you are traveling.




1.1 Features

- ✓ Create temporary, personal, wireless access in your hotel room or a coffee shop hotspot
- ✓ Travel size design with selectable extra 2dBi high gain dipole antenna to enhance performance
- ✓ High security with build-in: WEP 64/128, WPA, WPA2 mixed, 802.1x and 802.11i
- ✓ Support AP, Gateway and Client Mode
- ✓ Wireless Quality of Service (QoS) - 802.11e,WMM
- ✓ Support WPS (Push button/ Pin code)
- ✓ Slide switch to change mode (Gateway/AP/Client) easily.

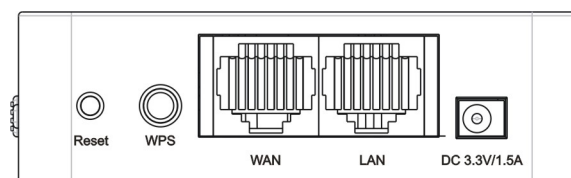
1.2 Physical Details

1.2.1 Front LEDs



LED Behavior				
LED	Printed	Color	Behavior	Indication
Power		Green	ON	Power on
			OFF	Power off
WPS		Green	ON	WPS function on
			OFF	WPS function off
			Blinking	WPS is enabled to make a connection
Wireless LAN		Green	OFF	WLAN off
			ON	WLAN link / active
			Blinking	WLAN traffic transmitting

1.2.2 Rear Panel



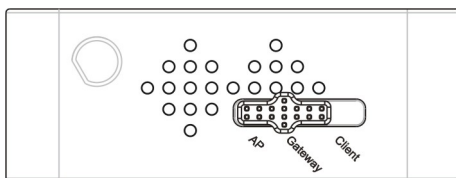
Reset	Keep on pressing the Reset button more than 3 seconds, the Wireless Portable Router will set all setting back to factory default values.
WPS	To enable the WPS function via web configuration (Wireless Settings> WPS), then press the WPS button once on the Wireless Portable Router, the GREEN LED will start to flash. To make a connection with other WPS supported device within 2 minutes.
WAN	Connect the ADSL or Cable Modem here with RJ45 cable. If your modem came with a cable, use the supplied cable, otherwise, use a standard LAN cable.
LAN	Use standard LAN cables (RJ45 connectors) to connect your PCs to the port. If required, any port can be connected to another hub. Any LAN port will automatically function as an "Uplink" port when necessary.
DC 3.3V/1.5A	Connect the power supply adapter here.

Chapter 2: About Operation Modes

This device provides operational applications with AP, Gateway and Client (Infrastructure) modes, which are mutually exclusive.

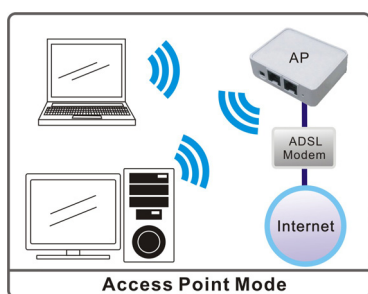
This device is shipped with configuration that is functional right out of the box. If you want to change the settings in order to perform more advanced configuration or even change the mode of operation, you can MANUALLY switch to the mode you desired by the manufacturer as described in the following sections.

2.1 Operation Modes



You have to MANUALLY switch the bar into the mode you preferred, AP, Gateway, or Client mode, then the device will reboot automatically into the mode you have selected.

2.2 Access Point Mode

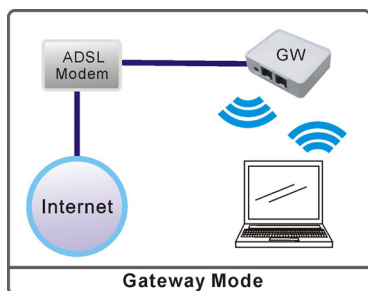


System Status

Let's take a look at the status of system.	
Internet	
Item	Status
Firmware Version	21.4.0.0.0.1e_b4 (Mar 24 2009)
System Up Time	54 secs
Operation Mode	AP Mode

When acting as an Access Point (AP), this device connects all the stations (PC/notebook with wireless network adapter) to a wireless network. All stations can have the Internet access if only the Access Point has the Internet connection.

2.3 Gateway Mode



System Status

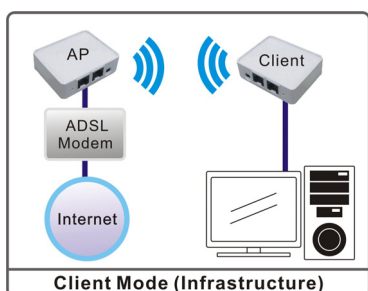
Let's take a look at the status of system.

Internet

Item	Status
Firmware Version	21.4.0.0.0.1e_b4 (Mar 24 2009)
System Up Time	27 secs
Operation Mode	Gateway Mode

When Gateway (GW) mode is selected, the device will enter gateway mode. And the wireless connection will be set up from a point-to-point local LAN into a point-to-multipoint WAN.

2.4 Client Mode



System Status

Let's take a look at the status of system.

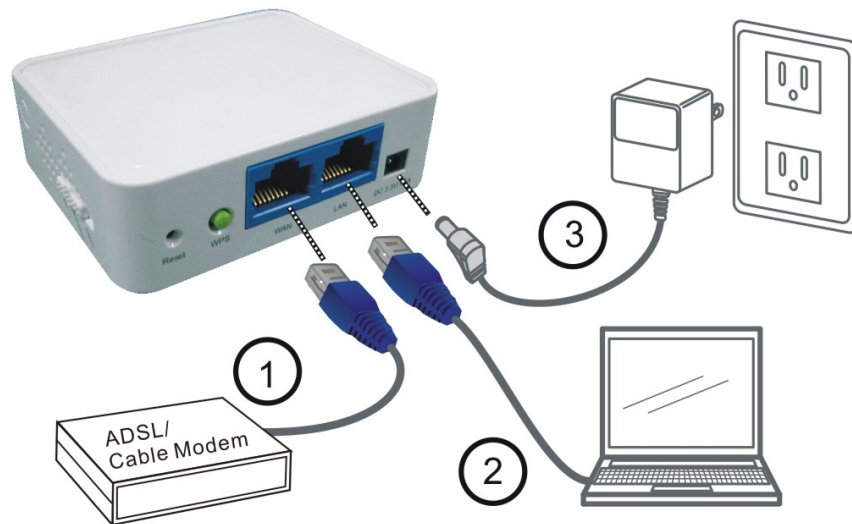
Internet

Item	Status
Firmware Version	21.4.0.0.0.1e_b4 (Mar 24 2009)
System Up Time	28 secs
Operation Mode	Client Mode

If set to Client (Infrastructure) mode, a device connects to each other through an access point or a base station (gateway or router.) This device can work like a wireless station when it's connected to a computer directly, so that the computer can send packets from wired end to wireless interface.

Chapter 3: Configuration

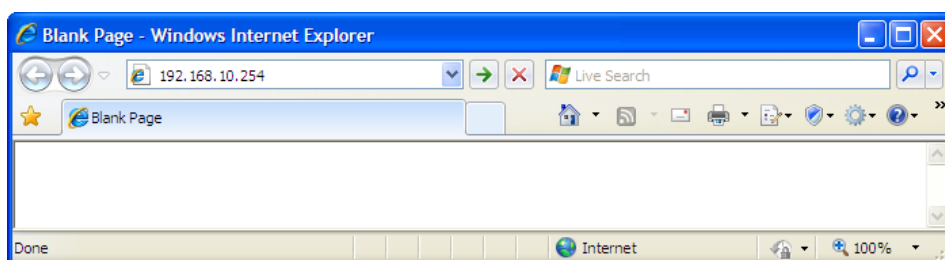
3.1 Hardware Connection



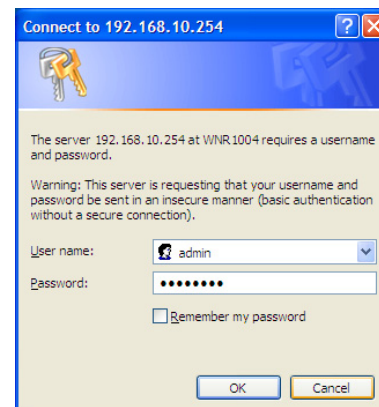
1. Connect one end of the Ethernet cable to the WAN port of the Wireless Portable Router, another end to the ADSL or cable modem.
2. Then, connect another Ethernet cable one end to the LAN port of the Wireless Portable Router, the other end to your PC or notebook.
3. Finally, connect the Wireless Portable Router with a power to an outlet.

3.2 Login

1. Start your computer and make sure the connection by an Ethernet cable between your computer and the Wireless-N Portable Router.
2. Start your Web Browser, eg: Internet Explorer,



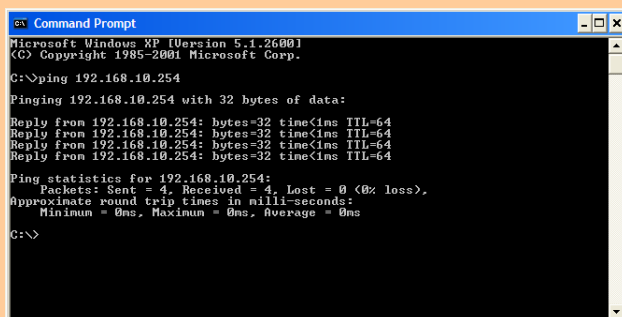
3. In the Address box, enter the IP address of the Wireless-N Portable Router, as in this example, which uses the Wireless-N Portable Router's default IP address: `http://192.168.10.254`
4. After connected successfully, the following screen will prompt up. Simply enter the username "admin" and password "admin" to login.



If you cannot connect...

If the Wireless-N Portable Router does not respond, check the following:

1. The Wireless Portable Router is properly installed, LAN connection is OK, and it is powered ON. You can test the connection by using the "Ping" command:
2. Open the MS-DOS window or command prompt window.
3. Enter the command: `ping 192.168.10.254`



If no response is received, either the connection is not working, or your PC's IP address is not compatible with the Wireless-N Portable Router's IP Address, continue with below checking:

1. If your PC is using a fixed IP Address, its IP Address must be within the range 192.168.10.1 to 192.168.10.253 to be compatible with the Wireless Portable Router's default IP Address of 192.168.10.254. Also, the Network Mask must be set to 255.255.255.0. See Chapter 4 - PC Configuration for details on checking your PC's TCP/IP settings.
2. Ensure that your PC and the Wireless Portable Router are on the same network segment. (If you don't have a router, this must be the case.)
3. Ensure you are using the wired LAN interface. The Wireless interface can only be used if its configuration matches your PC's wireless settings.

3.2.1 Common Connection Types

3.2.1.1 Cable Modems

Type	Details	ISP Data required
Dynamic IP Address	Your IP Address is allocated automatically, when you connect to you ISP.	Usually, none. However, some ISP's may require you to use a particular Hostname, Domain name, or MAC (physical) address.
Static (Fixed) IP Address	Your ISP allocates a permanent IP Address to you.	IP Address allocated to you. Some ISP's may also require you to use a particular Hostname, Domain name, or MAC (physical) address.

3.2.1.2 DSL Modems

Type	Details	ISP Data required
Dynamic IP Address	Your IP Address is allocated automatically, when you connect to you ISP.	None.
Static (Fixed) IP Address	Your ISP allocates a permanent IP Address to you.	IP Address allocated to you.
PPPoE	You connect to the ISP only when required. The IP address is usually allocated automatically.	User name and password.
PPTP	Mainly used in Europe. You connect to the ISP only when required. The IP address is usually allocated automatically, but may be Static (Fixed).	<ul style="list-style-type: none"> • PPTP Server IP Address. • User name and password. • IP Address allocated to you, if Static (Fixed).

3.2.1.3 Other Modems (e.g. Broadband Wireless)

Type	Details	ISP Data required
Dynamic IP Address	Your IP Address is allocated automatically, when you connect to you ISP.	None.
Static (Fixed) IP Address	Your ISP allocates a permanent IP Address to you.	IP Address allocated to you.

3.3 Wizard (Gateway Mode)

3.3.1 Step 1 – WAN Access Type

Here user can set up the WAN connection type easily. Select the WAN Connection Type Static IP, DHCP Client, PPPoE or L2TP, PPTP and click Next to continue.

Wide Area Network (WAN) Settings

You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.

WAN Connection Type:		DHCP (Auto config) ▼
DHCP Mode		
Hostname	<input type="text"/>	
MAC Clone		
Enabled	Disable ▼	
Apply		Cancel

3.3.1.1 DHCP Client

WAN Access Type:	DHCP Client ▼
<div> Cancel << Back Next >> </div>	

If the DHCP Client WAN connection be selected, the PC will obtain the IP address automatically.

3.3.1.2 Static IP

WAN Access Type:	Static IP ▼
IP Address	<input type="text" value="192.168.1.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text" value="192.168.1.254"/>
<div> Cancel << Back Next >> </div>	

If the Static IP be selected, user has to set up the IP address, subnet mask and default gateway according to the ISP that provided the related information.

IP Address : Enter the WAN IP address provided by your ISP here.

Subnet Mask : Enter the subnet mask here.

Default Gateway : Enter the default gateway IP address provided by your ISP here.

3.3.1.3 PPPoE

WAN Access Type:	PPPoE
User Name	pppoe_user
Password	••••••••

Cancel << Back Next >>

If the PPPoE be selected, user has to set up the user name and password according to the ISP that provided the related information.

User Name : Enter the username that provide by your ISP provider.

Password : Enter the password that provide by your ISP provider.

NOTE: Maximum input is 32 alphanumeric characters (case sensitive).

3.3.1.4 L2TP

WAN Access Type:	L2TP
L2TP Server IP Address	l2tp_server
User Name	l2tp_user
Password	••••••••

Cancel << Back Next >>

If the L2TP be selected, user has to set up the server IP address, user name and password according to the ISP that provided the related information.

L2TP Server IP Address : Enter the L2TP Server IP Address in this column.

User Name : Maximum input is 20 alphanumeric characters (case sensitive).

Password : Maximum input is 32 alphanumeric characters (case sensitive).

3.3.1.5 PPTP

WAN Access Type:	PPTP
PPTP Server IP Address	pptp_server
User Name	pptp_user
Password	••••••••

Cancel << Back Next >>

If the PPTP be selected, user has to set up the server IP address, user name and password according to the ISP that provided the related information.

PPTP Server IP Address : Enter the PPTP Server IP Address in this column.

User Name : Maximum input is 20 alphanumeric characters (case sensitive).

Password : Maximum input is 32 alphanumeric characters (case sensitive).

3.3.2 Step 2 – LAN

This step can set up Wireless Portable Router's IP address, subnet mask, DHCP type, DHCP IP addresses range, DHCP subnet mask and DHCP lease time.

Local Area Network (LAN) Settings

You may enable/disable networking functions and configure their parameters as your wish.

LAN Setup	
IP Address	192.168.10.254
Subnet Mask	255.255.255.0
MAC Address	00:12:0E:AF:13:A4
DHCP Type	Server ▼
Start IP Address	192.168.10.100
End IP Address	192.168.10.200
Subnet Mask	255.255.255.0
DHCP Primary DNS	192.168.10.254
DHCP Secondary DNS	0.0.0.0
Default Gateway	192.168.10.254
Lease Time	86400

IP Address	Shows the IP address of the Wireless Portable Router (Default IP address is 192.168.10.254.)
Subnet Mask	The subnet mask of the Wireless Portable Router (Default subnet mask is 255.255.255.0.)
DHCP Type	<p>Disable: Select to disable this Wireless Portable Router to distribute IP addresses to connected clients.</p> <p>Server: Select to enable this Wireless Portable Router to distribute IP Addresses (DHCP Server) to connected clients. And the following field will be activated for you to enter the starting IP Address.</p>
DHCP Start IP	The starting addresses of this local IP network address pool. The pool is a piece of continuous IP address segment. Keep the default value 192.168.10.100 should work for most cases.
DHCP End IP	The end IP address, the maximum is 253. Default value 253 should work for most cases (192.168.10.253.) If "Start IP Address" is set at 192.168.10.100 and the "End IP address" is 192.168.10.253, the device will distribute IP addresses from 192.168.10.100 to 192.168.10.253 to all the computers in the network that request IP addresses from DHCP server (Router).
DHCP Subnet Mask	The subnet mask of the distribute IP addresses clients, the subnet mask must be set at the same segment as the Wireless Portable Router.

DHCP Lease Time	The lease time of the distribute IP Addresses. Default settings are 86400 seconds.
-----------------	--

3.3.3 Step 3 – Network Mode

This step can set up wireless network mode, network name and channel.

Basic Wireless Settings

You could configure the minimum number of Wireless settings for communication, such as Network Name (SSID) and Channel. The Access Point can be set simply with only the minimum setting items.

Wireless Network	
Radio On/Off	<input type="button" value="RADIO OFF"/>
Network Mode	11b/g/n mixed mode ▼
Network Name(SSID)	PROLiNK_WNR1004

Network Mode	Select 11b/g mixed, 11b only, 11g only, or 11b/g/n mixed mode from the pull-down menu. (Default is 11b/g/n mixed mode.)
Network (SSID)	A SSID is referred to a network name because essentially it is a name that identifies a wireless network.
Frequency (Channel)	Select 1~11 or Auto Select from the pull-down menu.

3.3.4 Step 4 – Security

Here can set up the wireless security of the Wireless Portable Router.

Wireless Security/Encryption Settings

Setup the wireless security and encryption to prevent from unauthorized access and monitoring.

Select SSID	
SSID choice	PROLiNK_WNR1004 ▼

"PROLiNK_WNR1004"	
Security Mode	Disable ▼

Access Policy	
Policy	Disable ▼
Add a station Mac:	<input type="text"/>

Select desired security type from the pull-down menu Disable, OPEN, SHARED, WEP AUTO, WPA-PSK, WPA2-PSK, and WPA-PSK/WPA2-PSK. The default setting is Disable. It is strongly recommended to set up security mode (OPEN, SHARED, WEP AUTO, WPA-PSK, WPA2-PSK, WPA-PSK/WPA2-PSK) to prevent any unauthorized accessing.

3.4.4.1 OPEN/SHARED/WEP AUTO

Security Mode	OPEN	
Default Key		Key 1
WEP Key 1 :		Hex
WEP Key 2 :		Hex
WEP Key 3 :		Hex
WEP Key 4 :		Hex

Default Key : Select the default key Key1~4.

WEP Key 1~4 : Enter the key in the selected key field. Only valid when using WEP encryption algorithm. The key must match with the AP's key. There are several formats to enter the keys.

- Hexadecimal (WEP 64 bits) : 10 Hex characters (0~9, a~f).
- Hexadecimal (WEP 128 bits) : 26 Hex characters (0~9, a~f).
- ASCII (WEP 64 bits) : 5 ASCII characters (case-sensitive).
- ASCII (WEP 128 bits) : 13 ASCII characters (case-sensitive).

3.4.4.2 WPA-PSK/ WPA2-PSK/ WPA-PSK/WPA2-PSK

Security Mode	WPA2-PSK
WPA Algorithms	<input type="radio"/> TKIP <input checked="" type="radio"/> AES <input type="radio"/> TKIP/AES
Pass Phrase	12345678

WPA Algorithms : Select the type of algorithm, TKIP or AES for WP-PSK, and TKIP, AES or TKIP/AES for WPA2-PSK, WPA-PSK/WPA2- PSK.

Pass Phrase : Enter the pass phrase 8~63 ASCII or 64 HEX characters in the column.

3.4 Internet Settings

3.4.1 WAN (Gateway)

Wide Area Network (WAN) Settings

You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.

WAN Connection Type:		DHCP (Auto config) ▼
DHCP Mode		
Hostname	<input type="text"/>	
MAC Clone		
Enabled	Disable ▼	
Apply		Cancel

Select the WAN Connection Type Static (fixed IP), DHCP (Auto Config), PPPoE (ADSL) and L2TP, PPTP. Default setting is DHCP enabled.

3.4.1.1 DHCP (Auto Config)

WAN Connection Type:		DHCP (Auto config) ▼
DHCP Mode		
Hostname	<input type="text"/>	

Hostname : Enter the hostname that assigned IP address to user's computer in this field.
Maximum input is 32 alphanumeric characters (case sensitive).

3.4.1.2 Static (fixed IP)

WAN Connection Type:		STATIC (fixed IP) ▼
Static Mode		
IP Address	<input type="text"/>	
Subnet Mask	<input type="text"/>	
Default Gateway	<input type="text"/>	
Primary DNS Server	<input type="text"/>	
Secondary DNS Server	<input type="text"/>	

IP Address : Enter the WAN IP address provided by your ISP in this column.
Subnet Mask : Enter the Subnet Mask in this column.
Default Gateway : Enter the default gateway IP address provided by your ISP in this column.
Primary DNS Server : The DNS should be set to the address provided by your ISP.
Secondary DNS Server : The DNS should be set to the address provided by your ISP.

3.4.1.3 PPPoE (ADSL)

WAN Connection Type: PPPoE (ADSL)

PPPoE Mode	
User Name	pppoe_user
Password	••••••••
Verify Password	••••••••

User Name : Enter the username that provide by your ISP.

Maximum input is 32 alphanumeric characters (case sensitive).

Password : Enter the password that provide by your ISP.

Maximum input is 32 alphanumeric characters (case sensitive).

Verify Password : To confirm the password, please enter the same password in the filed again.

3.4.1.4 L2TP

WAN Connection Type: L2TP

L2TP Mode	
Server IP	l2tp_server
User Name	l2tp_user
Password	••••••••
Address Mode	Static
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254

Server IP: Enter the L2TP Server IP Address in this column.

User Name : Maximum input is 32 alphanumeric characters (case sensitive).

Password : Maximum input is 32 alphanumeric characters (case sensitive).

Address Mode : Select Dynamic or Static IP address mode for the pull-down menu.

IP Address : Enter the WAN IP address provided by your ISP in this column.

Subnet Mask : Enter the subnet mask in this column.

Default Gateway : Enter the default gateway IP address provided by your ISP in this column.

3.4.1.5 PPTP

WAN Connection Type: PPTP

PPTP Mode	
Server IP	pptp_server
User Name	pptp_user
Password	••••••~•
Address Mode	Static
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254

Server IP : Enter the L2TP Server IP Address in this column.

User Name : Maximum input is 32 alphanumeric characters (case sensitive).

Password : Maximum input is 32 alphanumeric characters (case sensitive).

- Address Mode : Select Dynamic or Static IP address mode for the pull-down menu.
- IP Address : Enter the WAN IP address provided by your ISP in this column.
- Subnet Mask : Enter the subnet mask in this column.
- Default Gateway : Enter the default gateway IP address provided by your ISP in this column.

3.4.1.6 MAC Clone



Your ISP may require a particular MAC address in order for you to connect to the Internet. This MAC address is the PC's MAC address that your ISP had originally connected your Internet connection to. Type in or click Fill my MAC to replace the WAN MAC address with the MAC address of that PC.

Default setting is Disable. User can select Enable from the pull-down list, and click Fill my MAC button to fill in your PC's MAC address in the blank field.

3.4.2 LAN

Local Area Network (LAN) Settings

You may enable/disable networking functions and configure their parameters as your wish.

LAN Setup	
IP Address	192.168.10.254
Subnet Mask	255.255.255.0
MAC Address	00:12:0E:AF:13:A4
DHCP Type	Server
Start IP Address	192.168.10.100
End IP Address	192.168.10.200
Subnet Mask	255.255.255.0
DHCP Primary DNS	192.168.10.254
DHCP Secondary DNS	0.0.0.0
Default Gateway	192.168.10.254
Lease Time	86400
Statically Assigned	MAC: 00:00:00:00:00:00 IP: 0.0.0.0
Statically Assigned	MAC: 00:00:00:00:00:00 IP: 0.0.0.0
Statically Assigned	MAC: 00:00:00:00:00:00 IP: 0.0.0.0
802.1d Spanning Tree	Disable
LLTD	Disable
UPNP	Disable
PPPoE Relay	Disable
DNS Proxy	Enable
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

IP Address

Shows the IP address of the Wireless Portable Router (Default IP address is 192.168.10.254.)

Subnet Mask

The subnet mask of the Wireless Portable Router (Default subnet mask is 255.255.255.0.)

MAC Address

Shows the MAC address of this Wireless Portable Router.

DHCP Type

Disable: Select to disable this Wireless Portable Router to distribute IP addresses to connected clients.

Server: Select to enable this Wireless Portable Router to distribute IP Addresses (DHCP Server) to connected clients. And the following field will be activated for you to enter the starting IP Address.

Start IP Address

The starting addresses of this local IP network address pool. The pool is a piece of continuous IP address segment. Keep the default value 192.168.10.100 should work for most cases.

End IP address

The end IP address, the maximum is 253. Default value 253 should work for most cases (192.168.10.253.) If "Start IP Address" is set at 192.168.10.100 and the "End IP address" is 192.168.10.253, the device will distribute IP addresses from

192.168.10.100 to 192.168.10.253 to all the computers in the network that request IP addresses from DHCP server (Router).

Subnet Mask The subnet mask of the distribute IP addresses clients, the subnet mask must be set at the same segment as the Wireless Portable Router.

Primary DNS Server Enter the DNS server IP address(es) that provided by your ISP, or you can specify your own preferred DNS server IP address(es).

Secondary DNS Server Secondary DNS Server is optional. You can enter another DNS server's IP address as a backup.

Default Gateway Shows the default gateway IP address.

Lease Time The lease time of the distribute IP Addresses. Default settings are 86400 seconds.

Statically Assigned MAC: Enter the MAC address of a certain station, and then the DHCP Server will to distribute a fixed IP address to the station automatically once be connected.
IP: Enter the fixed IP address that DHCP Server assigned to a certain connected station.

User can set up 3 set of fixed IP addresses that distribute form the Wireless Portable Router when the DHCP Type function be selected to Server.

802.1d Spanning Tree Select Enabled or Disabled from the pull-down menu.

LLTD Link Layer Topology Discovery (LLTD) is a proprietary Link Layer protocol for network topology discovery and quality of service diagnostics. The LLTD protocol operates over both wired (IEEE 802.3 Ethernet) as well as wireless (IEEE 802.11) networks.

LLTD is included in Windows Vista and is used by its Network Map feature to display a graphical representation of the LAN or WLAN, to which the computer is connected. Windows XP does not contain the LLTD protocol as a standard component and as a result, Windows XP computers do not appear on the Network Map unless the LLTD responder is installed on Windows XP computers.

Select Enabled or Disabled from the pull-down menu.

IGMP Proxy The Internet Group Management Protocol (IGMP) is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships.

Select Disable or Enable from the pull-down menu.

UPNP Universal Plug and Play (UPnP) is a set of computer protocols promulgated by the UPnP Forum. The goals of UPnP are to allow devices to connect seamlessly and to

simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components. UPnP achieves this by defining and publishing UPnP device control protocols built upon open, Internet-based communication standards. The term UPnP is derived from plug-and-play, a technology for dynamically attaching devices directly to a computer.

Select Disable or Enable from the pull-down menu.

PPPoE Relay

Select Disable or Enable from the pull-down menu.

DNS Proxy

Select Disable or Enable from the pull-down menu.

Apply

After completing the settings on this page, click Apply button to save the settings.

Cancel

Click Cancel to restore to default values.

3.4.3 DHCP Clients

DHCP Client List

You could monitor DHCP clients here.

DHCP Clients		
MAC Address	IP Address	Expires in
00:16:D3:2E:AE:87	192.168.10.100	23:53:40
00:12:0E:A8:FE:B8	192.168.10.101	00:00:00
00:25:47:EA:D9:38	192.168.10.102	00:00:00
00:12:0E:9F:2B:24	192.168.10.103	00:00:00
00:25:47:EA:DC:EB	192.168.10.104	00:00:00
00:16:6F:2C:32:E7	192.168.10.105	00:00:00
00:23:4D:AD:5B:5C	192.168.10.106	00:00:00
00:1C:D4:F5:3A:1B	192.168.10.107	21:31:04
00:12:F0:B3:43:88	192.168.10.108	18:38:00

Here shows the IP assigned clients that computer in the network requests IP addresses from DHCP server (Wireless Portable Router).

3.4.4 VPN Passthrough (Gateway Mode)

VPN Passthrough

VPN passthrough configurations including: L2TP, IPSec, and PPTP passthrough.

VPN Pass Through	
L2TP Passthrough	Disable ▾
IPSec Passthrough	Disable ▾
PPTP Passthrough	Disable ▾

Apply Cancel

VPN passthrough configurations including: L2TP, IPSec, and PPTP passthrough.

L2TP Passthrough L2TP, Layer Two Tunneling Protocol (L2TP). Use the L2TP with VPN that user can access the personal network via Internet.

Select Enabled or Disabled from the pull-down menu.

IPSec Passthrough IPSec, Internet Protocol Security. Select Enabled or Disabled from the pull-down menu.

PPTP Passthrough PPTP, Point-to-Point Tunneling Protocol. Select Enabled or Disabled from the pull-down menu.

3.4.5 Advanced Routing (Gateway Mode)

If you connect several routers with this Wireless Portable Router, you may need to set up a predefined routing rule to have more effective network topology/traffic, this is called static route between those routers and the Wireless Portable Router.

To set static routers, enter the settings including route IP address, route mask route gateway the route Interface from LAN or WAN.

Static Routing Settings

You may add and remote custom Internet routing rules, and/or enable dynamic routing exchange protocol here.

Add a routing rule									
Destination	<input type="text"/>								
Range	Host <input type="button" value="v"/>								
Gateway	<input type="text"/>								
Interface	LAN <input type="button" value="v"/> <input type="text"/>								
Comment	<input type="text"/>								
<input type="button" value="Apply"/> <input type="button" value="Reset"/>									

Current Routing table in the system:									
No.	Destination	Netmask	Gateway	Flags	Metric	Ref	Use	Interface	Comment
1	255.255.255.255	255.255.255.255	0.0.0.0	5	0	0	0	LAN (br0)	
2	10.10.10.0	255.255.255.0	0.0.0.0	1	0	0	0	LAN (br0)	

Dynamic Routing Settings

Dynamic Routing Protocol	
RIP	Disable <input type="button" value="v"/>
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

Destination	The network address of the destination LAN segment. When a packet with destination IP address that matches to this field, it will route to the device set in the Route Gateway field.
Range	Select Host or Net from the pull-down menu.
Gateway	Enter the Gateway IP address in the field.
Interface	You can select to use LAN, WAN or Custom as the physical interface from where the packets will be sent.
Comment	Enter note or remark here.
Dynamic Routing Settings	Select Disable or Enable form pull-downm list to use the RIP function.
Apply	After completing the settings on this page, click Apply button to save the settings.
Reset	Click to discard current setting.

3.4.6 QoS

Quality of Service Settings

You may setup rules to provide Quality of Service guarantees for specific applications.

QoS Setup	
Quality of Service	Disable ▾
Upload Bandwidth:	User defined ▾ <input type="text"/> Bits/sec
Download Bandwidth:	User defined ▾ <input type="text"/> Bits/sec
<input type="button" value="Submit"/>	

Quality of Service Select Disable or Enable from the pull-down menu. (Default setting is Disable.)

Upload Bandwidth Select User defined to enter the upload transmitting bandwidth bits/sec in the blank or select the upload bandwidth from pull-down list.

Download Bandwidth Select User defined to enter the download transmitting bandwidth bits/sec in the blank or select the download bandwidth from pull-down list.

3.5 Wireless Settings

3.5.1 Gateway / Access Point Modes

3.5.1.1 Basic Wireless Settings

Basic Wireless Settings

You could configure the minimum number of Wireless settings for communication, such as Network Name (SSID) and Channel. The Access Point can be set simply with only the minimum setting items.

Wireless Network	
Radio On/Off	<input type="button" value="RADIO OFF"/>
Network Mode	11b/g/n mixed mode ▾
Network Name(SSID)	RT3052_AP
Multiple SSID1	<input type="text"/>
Multiple SSID2	<input type="text"/>
Multiple SSID3	<input type="text"/>
Multiple SSID4	<input type="text"/>
Multiple SSID5	<input type="text"/>
Multiple SSID6	<input type="text"/>
Multiple SSID7	<input type="text"/>
Broadcast Network Name (SSID)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
MBSSID AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
BSSID	00:0C:43:30:50:88
Frequency (Channel)	2437MHz (Channel 6) ▾
HT Physical Mode	
Operating Mode	<input checked="" type="radio"/> Mixed Mode <input type="radio"/> Green Field
Channel BandWidth	<input type="radio"/> 20 <input checked="" type="radio"/> 20/40
Guard Interval	<input type="radio"/> Long <input checked="" type="radio"/> Auto
MCS	Auto ▾
Reverse Direction Grant(RDG)	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Extension Channel	2457MHz (Channel 10) ▾
Aggregation MSDU(A-MSDU)	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Auto Block ACK	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Decline BA Request	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Other	
HT TxStream	2 ▾
HT RxStream	2 ▾

Wireless Network

Radio On/Off

Click Radio ON/OFF button to turn on/off the radio function.

Network Mode

Select 11b/g mixed, 11b only, 11g only, or 11b/g/n mixed mode from the pull-down menu. (Default is 11b/g/n mixed mode.)

Network Name (SSID)

A SSID is referred to a network name because essentially it is a name that identifies a wireless network.

Multiple SSID 1~7

A multiple SSID is referred to a network name because essentially it is a name that identifies a wireless network.

Broadcast Network Name(SSID)	<p>Enable: This wireless AP will broadcast its SSID to stations.</p> <p>Disable: This wireless AP will not broadcast its SSID to stations. If stations want to connect to this wireless AP, this AP's SSID should be known in advance to make a connection.</p>
AP Isolation	Select Enable or Disable to enable this function.
MBSSID AP Isolation	Select Enable or Disable to enable this function.
BSSID	Shows the MAC address of the Wireless Portable Router.
Frequency (Channel)	Select 1~11 or Auto Select from the pull-down menu.
HT Physical Mode	
Operating Mode	Green Field (11n mode), Mixed Mode(11b/g/n mode). Select Mixed Mode or Green Field. (Default operating mode is Mixed Mode.)
Channel Band Width	Select 20 or 20/40. (Default setting is 20/40.)
Guard Interval	Select Long or Auto. (Default setting is Auto.)
MCS	Select form the pull-down menu 0~15, 32 or Auto. (Default setting is Auto.)
Reverse Direction Grant(RDG)	Select Disable or Enable this function. (Default setting is Enable.)
Extension Channel	You can select 2457MHz (Channel 10) or 2417MHz (Channel 2) form the pull-down menu.
Aggregation MSDU (A-MSDU)	Select Disable or Enable. (Default setting is Disable.)
Auto Block ACK	Select Disable or Enable. (Default setting is Enable.)
Decline BA Request	Select Disable or Enable. (Default setting is Disable.)
Other	
HT Tx Stream	Select 1 or 2 form the pull-down menu.
HT Rx Stream	Select 1 or 2 form the pull-down menu.
Apply	Click to save and apply the current settings.
Cancel	Click to discard the current settings.

3.5.1.2 Advanced Wireless Settings

Advanced Wireless Settings

Use the Advanced Setup page to make detailed settings for the Wireless. Advanced Setup includes items that are not available from the Basic Setup page, such as Beacon Interval, Control Tx Rates and Basic Data Rates.

Advanced Wireless	
BG Protection Mode	Auto <input type="button" value="v"/>
Beacon Interval	100 ms (range 20 - 999, default 100)
Data Beacon Rate (DTIM)	1 ms (range 1 - 255, default 1)
Fragment Threshold	2346 (range 256 - 2346, default 2346)
RTS Threshold	2347 (range 1 - 2347, default 2347)
TX Power	100 (range 1 - 100, default 100)
Short Preamble	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Short Slot	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Tx Burst	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Pkt_Aggregate	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
IEEE 802.11H Support	<input type="radio"/> Enable <input checked="" type="radio"/> Disable (only in A band)
Country Code	None <input type="button" value="v"/>

Wi-Fi Multimedia	
WMM Capable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
APSD Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
DLS Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
WMM Parameters	<input type="button" value="WMM Configuration"/>

Multicast-to-Unicast Converter	
Multicast-to-Unicast	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Advanced Wireless

BG Protection Mode

Select the protection mode from the pull-down list, Auto, On and Off.

Beacon Interval

Beacon Interval is the amount of time between beacon transmissions. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon. Range 20-999. (Default Beacon Interval is 100.)

Data Beacon Rate (DTIM)

Range from 1 to 255. (Default data beacon rate is 1.)

Fragment Threshold

Fragmentation mechanism is used for improving the efficiency when high traffic flows along in the wireless network. If the Wireless Portable Router often transmits large files in wireless network, you can enter new Fragment Threshold value to split the packet. The value can be set from 256 to 2346. (The default value is 2346.)

RTS Threshold

RTS Threshold is a mechanism implemented to prevent the "Hidden Node" problem. If the "Hidden Node" problem is an issue, please specify the packet size. The RTS mechanism will be activated if the data size exceeds the value you set. (The default value is 2347.)

Warning: Enabling RTS Threshold will cause redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

This value should remain at its default setting of 2347. Should you encounter inconsistent data flow, only minor modifications of this value are recommended.

Short Preamble

Select Disable or Enable this function. (Default setting is Disable.) A preamble is a signal used in wireless environment to synchronize the transmitting timing including Synchronization and Start frame delimiter.

Short Slot

Select Disable or Enable this function. (Default short slot setting is Enable.)

Tx Burst

Check the box to enable the Tx Burst function. (Default Tx Burst setting is Enable.)

Pkt_Aggregate

Select Disable or Enable this function. (Default setting is Enable.)

Wi-Fi Multimedia**WMM Capable**

WMM Power Save is a set of features for Wi-Fi networks that help conserve battery power in small devices such as phones, PDAs, and audio players. The certification for both access points and client devices uses mechanisms from the recently ratified IEEE 802.11e standard, and is an enhancement of legacy 802.11 power saves. WMM Power Save helps pave the way for rapid proliferation of Wi-Fi technology into devices dependent on battery power.

Select Disable or Enable to use or stop Wi-Fi Multimedia function. (Default setting is Enable.)

APSD Capable

Automatic Power Save Delivery is a more efficient power management method than legacy 802.11 Power Save Polling. Most new 802.11 stations already support a power management mechanism similar to APSD. APSD is very useful for a VoIP phone, as data rates are roughly the same in both directions. Whenever Voice data are sent to the Access Point, the Access Point is triggered to send the buffered Voice data in the other direction. After that the Voice over IP phone enters doze state until next Voice data have to be sent to the Access Point.

Select Disable or Enable this function. (Default setting is Disable.)

DLS Capable

Direct Link Setup, this function will be enabled under the connection with AP which must support the DLS function. Direct Link Setup allows direct STA-to-STA frame transfer within a BSS (Basic Service Set). This is designed for consumer use, where STA-to-STA transfer is more commonly used.

Select Disable or Enable this function. (Default setting is Disable.)

WMM Parameters

Click the WMM Configuration button to go further settings.

WMM Parameters of Access Point						
	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_BK	7	15	1023	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_VI	1	7	15	94	<input type="checkbox"/>	<input type="checkbox"/>
AC_VO	1	3	7	47	<input type="checkbox"/>	<input type="checkbox"/>

WMM Parameters of Station					
	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	1023	0	<input type="checkbox"/>
AC_BK	7	15	1023	0	<input type="checkbox"/>
AC_VI	2	7	15	94	<input type="checkbox"/>
AC_VO	2	3	7	47	<input type="checkbox"/>

Multicast-to-Unicast Converter

Multicast-to-Unicast Select Disable or Enable this function. (Default setting is Disable.)

3.5.1.3 Wireless Security/Encryption Settings

Wireless Security/Encryption Settings

Setup the wireless security and encryption to prevent from unauthorized access and monitoring.

Select SSID	
SSID choice	RT3052_AP

"RT3052_AP"	
Security Mode	Disable

Access Policy	
Policy	Disable
Add a station Mac:	

Security Mode

There are eleven type of authentication modes including **Disable, Open, Shared, WEP Auto, WPA, WPA-PSK, WPA2, WPA2-PSK, WPA-PSK/ WPA2-PSK, WPA/WPA2 and 802.1X**. The security default setting is Disable.

Note:

- WPA and WPA-PAK only support TKIP and AES as encryption method.
- SHARED only supports WEP as encryption method.
- WEP AUTO means AP can accept STA connect to it using OPEN-WEP or SHARED-WEP.

a) OPEN/ WEP AUTO

If your wireless router is using **OPEN** or **WEP AUTO** authentication, then the wireless adapter will need to be set to the same authentication type.

Security Mode	OPEN	
Wire Equivalence Protection (WEP)		
Default Key	Key 1	
WEP Key 1 :	<input type="text"/>	Hex
WEP Key 2 :	<input type="text"/>	Hex
WEP Key 3 :	<input type="text"/>	Hex
WEP Key 4 :	<input type="text"/>	Hex

Default Key Select the default key.

WEP Key 1~4 Enter the key in the selected key field. Only valid when using WEP encryption algorithm. The key must match with the AP's key. There are several formats to enter the keys.

- Hexadecimal (WEP 64 bits) : 10 Hex characters (0~9, a~f).
- Hexadecimal (WEP 128 bits) : 26 Hex characters (0~9, a~f).
- ASCII (WEP 64 bits) : 5 ASCII characters (case-sensitive).
- ASCII (WEP 128 bits) : 13 ASCII characters (case-sensitive).

b) Shared

Shared key is when both the sender and the recipient share a secret key.

Security Mode	SHARED	
Encrypt Type	WEP	
Wire Equivalence Protection (WEP)		
Default Key	Key 1	
WEP Key 1 :	<input type="text"/>	Hex
WEP Key 2 :	<input type="text"/>	Hex
WEP Key 3 :	<input type="text"/>	Hex
WEP Key 4 :	<input type="text"/>	Hex

Encryption Type The encryption type is WEP.

Default Key Select the default key.

WEP Key 1~4 Enter the key in the selected key field. Only valid when using WEP encryption algorithm. The key must match with the AP's key. There are several formats to enter the keys.

- Hexadecimal (WEP 64 bits) : 10 Hex characters (0~9, a~f).
- Hexadecimal (WEP 128 bits) : 26 Hex characters (0~9, a~f).
- ASCII (WEP 64 bits) : 5 ASCII characters (case-sensitive).
- ASCII (WEP 128 bits) : 13 ASCII characters (case-sensitive).

WPA2, WPA2-PSK, WPA-PSK/WPA2-PSK, and WPA1 WPA2 offer three encryption methods, TKIP, AES and TKIP AES.

c) WPA/WPA2/WPA1 WPA2

Security Mode	WPA
WPA	
WPA Algorithms	<input type="radio"/> TKIP <input type="radio"/> AES <input type="radio"/> TKIPAES
Key Renewal Interval	3600 seconds
Radius Server	
IP Address	
Port	1812
Shared Secret	
Session Timeout	0
Idle Timeout	

WPA Algorithms

Select the type of algorithm, TKIP or AES for WPA, and TKIP, AES or TKIP AES for WPA2, WPA1/WPA2.

Key Renewal

Enter the renewal security time (seconds) in the column. Default is 3600 seconds. Set 0 to disable re-key.

Interval**RADIUS Server**

RADIUS is an authentication, authorization and accounting client-server protocol.

The client is a Network Access Server that desires to authenticate its links. The server is a server that has access to a user database with authentication information.

IP Address

Enter the RADIUS Server's IP Address provided by your ISP.

Port

Enter the RADIUS Server's port number provided by your ISP. (The default is 1812.)

Shared Secret

Enter the password that the Wireless Portable Router shares with the RADIUS Server.

Session Timeout

Session timeout interval is for 802.1x re-authentication setting. Set to zero to disable 802.1x re-authentication service for each session. Session timeout interval unit is second and must be larger than 60.

Idle Timeout

Enter the idle timeout in the column.

PMK Cache Period

Only valid in WPA2 security. Set WPA2 PMKID cache timeout period, after time out, the cached key will be deleted. PMK Cache Period unit is minute.

Pre-Authentication

Only valid in WPA2 security. The most important features beyond WPA to become standardized through 802.11i/WPA2 are pre-authentication, which enables secure fast roaming without noticeable signal latency.

d) WPA-PSK/WPA2-PSK/WPA-PSK WPA2-PSK

Security Mode	WPA-PSK
WPA	
WPA Algorithms	<input type="radio"/> TKIP <input type="radio"/> AES <input type="radio"/> TKIPAES
Pass Phrase	12345678
Key Renewal Interval	3600 seconds

WPA Algorithms

Select the type of algorithm, TKIP or AES for WP-PSK, and TKIP, AES or TKIP AES for WPA2-PSK, WPA1 PSK WPA2 PSK.

Pass Phrase

Enter the pass phrase 8~63 ASCII or 64 HEX characters in the column.

Key Renewal Interval

Enter the renewal security time (seconds) in the column. Default is 3600 seconds. Set 0 to disable re-key.

e) 802.1x

Security Mode	802.1X
802.1x WEP	
WEP	<input type="radio"/> Disable <input type="radio"/> Enable
Radius Server	
IP Address	
Port	1812
Shared Secret	
Session Timeout	
Idle Timeout	

WEP

Select Disable or Enable to this function.

RADIUS Server

RADIUS is an authentication, authorization and accounting client-server protocol. The client is a Network Access Server that desires to authenticate its links. The server is a server that has access to a user database with authentication information.

IP Address

Enter the RADIUS Server's IP Address provided by your ISP.

Port

Enter the RADIUS Server's port number provided by your ISP. (The default is 1812.)

Shared Secret

Enter the password that the Wireless Portable Router shares with the RADIUS Server.

Session Timeout

Session timeout interval is for 802.1x re-authentication setting. Set to zero to disable 802.1x re-authentication service for each session. Session timeout interval unit is second and must be larger than 60.

Idle Timeout

Enter the idle timeout in the column.

Access Policy**Policy**

Set access control policy of the stations. Select Disable, Allow or Reject form the pull-down menu.

Add a station Mac

Enter a station MAC in the blank field.

3.5.1.4 Wireless Distribution System

Wireless Distribution System



Wireless Distribution System Settings.

Wireless Distribution System(WDS)

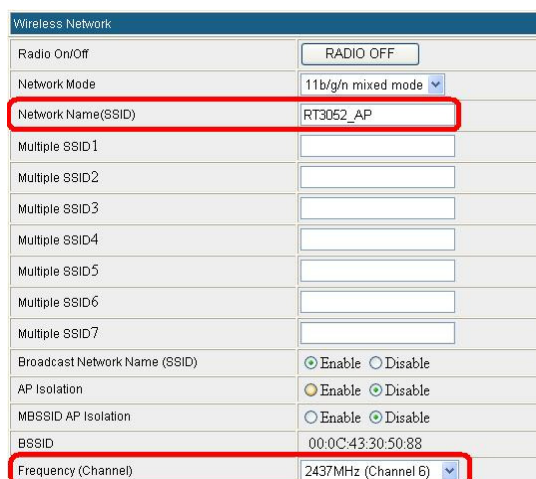
WDS Mode: Disable

Buttons: Apply, Cancel

Select the mode from the pull-down menu, Disable, Lazy Mode, Bridge Mode or Repeater Mode. (Default WDS mode is Disable.)

If the users would like to set up the WDS function, please go to Wireless settings> Basic to set up APs that should use the same SSID and Channel , then go back to Wireless settings> WDS to enter Wireless MAC of each other to make the WDS connection.

Step 1: Setup the same SSID and Channel on both wireless APs.



Wireless Network

Radio On/Off: RADIO OFF

Network Mode: 11b/g/n mixed mode

Network Name(SSID): RT3052_AP

Multiple SSID1:

Multiple SSID2:

Multiple SSID3:

Multiple SSID4:

Multiple SSID5:

Multiple SSID6:

Multiple SSID7:

Broadcast Network Name (SSID): ☒ Enable ☐ Disable

AP Isolation: ☐ Enable ☒ Disable

MBSSID AP Isolation: ☐ Enable ☒ Disable

BSSID: 00:0C:43:30:50:88

Frequency (Channel): 2437MHz (Channel 6)

Step 2: Enter Wireless MAC address to each other (according to the WDS mode that user selected).

a) Lazy Mode

If Lazy mode be selected, it is unnecessary to set up wireless MAC here, just go to set up Wireless MAC address on the other wireless AP then WDS function will be active.

Phy Mode

Select CCK(11b mode), OFDM(11g mode), HTMIX(11b/g/n mixed mode) or GREENFIELD(11n mode) from the pull-down menu. Each AP should be setup to the same Phy mode.

AP1~AP4 Encrypt Type

Users should go to the main web page of the Wireless Portable Router Wireless settings > Security page to set up security mode under Open, Shared, WEP Auto, WPA, WPA-PSK, WPA2, WPA2-PSK, WPA-PSK/ WPA2-PSK, WPA/WPA2.

Select NONE, WEP, TKIP and AES encryption type from pull-down menu. (Default encryption type is NONE.)

Encrypt Key

Enter the corresponding encryption keys in the field.

Select the type of Open, Shared, WEP Auto authentication, for WEP encryption.

- Hexadecimal (WEP 64 bits) : 10 Hex characters (0~9, a~f).
- Hexadecimal (WEP 128 bits) : 26 Hex characters (0~9, a~f).
- ASCII (WEP 64 bits) : 5 ASCII characters (case-sensitive).
- ASCII (WEP 128 bits) : 13 ASCII characters (case-sensitive).

Select the type WPA, WPA-PSK, WPA2, WPA2-PSK, WPA-PSK/ WPA2-PSK, WPA/WPA2 authentication, for TKIP or AES encryption.

If users select TKIP or AES encryption, please enter the password in the Encryption Key column that must be filled with characters longer than 8 and less than 64 lengths to set up the security.

b) Bridge Mode

If the Bridge mode be selected, set up Wireless MAC address to each other to enable WDS function.

Wireless Distribution System

Wireless Distribution System(WDS)	
WDS Mode	Bridge Mode
Phy Mode	CCK
AP1 EncryptType	NONE
Encrypt Key	
AP2 EncryptType	NONE
Encrypt Key	
AP3 EncryptType	NONE
Encrypt Key	
AP4 EncryptType	NONE
Encrypt Key	
AP1 MAC Address	
AP2 MAC Address	
AP3 MAC Address	
AP4 MAC Address	

Apply Cancel

Phy Mode

Select CCK, OFDM, HTMIX or GREENFIELD from the pull-down menu. Each AP should be setup to the same Phy mode.

AP1~AP4 Encrypt Type

Users should go to the main web page of the Wireless Portable Router Wireless settings > Security page to set up security mode under Open, Shared, WEP Auto, WPA, WPA-PSK, WPA2, WPA2-PSK, WPA-PSK/ WPA2-PSK, WPA/WPA2.

Select NONE, WEP, TKIP and AES encryption type from pull-down menu. (Default encryption type is NONE.)

Encrypt Key

Enter the corresponding encryption keys in the field.

Select the type of Open, Shared, WEP Auto authentication, for WEP encryption.

- Hexadecimal (WEP 64 bits) : 10 Hex characters (0~9, a~f).
- Hexadecimal (WEP 128 bits) : 26 Hex characters (0~9, a~f).
- ASCII (WEP 64 bits) : 5 ASCII characters (case-sensitive).
- ASCII (WEP 128 bits) : 13 ASCII characters (case-sensitive).

Select the type WPA, WPA-PSK, WPA2, WPA2-PSK, WPA-PSK/ WPA2-PSK, WPA/WPA2 authentication, for TKIP or AES encryption.

If users select TKIP or AES encryption, please enter the password in the Encryption Key column that must be filled with characters longer than 8 and less than 64 lengths to set up the security.

AP1~AP4 MAC Address

Enter Wireless MAC of each other to make the WDS connection.

c) Repeater Mode

If the Repeater mode be selected, set up Wireless MAC address to each other to enable WDS function.

Wireless Distribution System

Wireless Distribution System Settings.

Wireless Distribution System(WDS)	
WDS Mode	Repeater Mode
Phy Mode	CCK
AP1 EncryptType	NONE
Encrypt Key	
AP2 EncryptType	NONE
Encrypt Key	
AP3 EncryptType	NONE
Encrypt Key	
AP4 EncryptType	NONE
Encrypt Key	
AP1 MAC Address	
AP2 MAC Address	
AP3 MAC Address	
AP4 MAC Address	

Phy Mode

Select CCK, OFDM, HTMIX or GREENFIELD from the pull-down menu. Each AP should be setup to the same Phy mode.

AP1~AP4 Encrypt Type

Users should go to the main web page of the Wireless Portable Router Wireless settings > Security page to set up security mode under Open, Shared, WEP Auto, WPA, WPA-PSK, WPA2, WPA2-PSK, WPA-PSK/ WPA2-PSK, WPA/WPA2.

Select NONE, WEP, TKIP and AES encryption type from pull-down menu. (Default encryption type is NONE.)

Encrypt Key

Enter the corresponding encryption keys in the field.

Select the type of Open, Shared, WEP Auto authentication, for WEP encryption.

- Hexadecimal (WEP 64 bits) : 10 Hex characters (0~9, a~f).
- Hexadecimal (WEP 128 bits) : 26 Hex characters (0~9, a~f).
- ASCII (WEP 64 bits) : 5 ASCII characters (case-sensitive).
- ASCII (WEP 128 bits) : 13 ASCII characters (case-sensitive).

Select the type WPA, WPA-PSK, WPA2, WPA2-PSK, WPA-PSK/ WPA2-PSK, WPA/WPA2 authentication, for TKIP or AES encryption.

If users select TKIP or AES encryption, please enter the password in the Encryption Key column that must be filled with characters longer than 8 and less than 64 lengths to set up the security.

AP1~AP4 MAC Address

Enter Wireless MAC of each other to make the WDS connection.

3.5.1.5 Wi-Fi Protected Setup

Wi-Fi Protected Setup

You could setup security easily by choosing PIN or PBC method to do Wi-Fi Protected Setup.

WPS Config

WPS:

WPS Summary

WPS Current Status:	Idle
WPS Configured:	No
WPS SSID:	RT3052_AP
WPS Auth Mode:	Open
WPS Encryp Type:	None
WPS Default Key Index:	1
WPS Key(ASCII)	
AP PIN:	31663441

WPS Progress

WPS mode: ☒ PIN ☐ PBC

PIN:

WPS Status

WPS: Idle

WPS Config

WPS

Select Enable then click Apply to use WPS (Wi-Fi Protected Setup) function, then push physical WPS button on Wireless Portable Router to make a WPS connection. Default setting is Disable.

WPS Summary

WPS Current Status

After enabling the WPS function, if there is connection the status will show Configured, otherwise, the status will show Idle.

WPS Configured

Trigger WPS AP to do simple config with WPS Client. If WPS configured, here shows Yes, otherwise, NO.

WPS SSID

Shows the Wireless Portable Router network name.

WPS Auth Mode

The WPS authentication type supports Open, Shared, WEP Auto, WPA-PSK, WPA2, WPA2-PSK, WPA-PSK/ WPA2-PSK. Please go to the configuration page Wireless Settings > Security to set up the WPS security.

WPS Encryp Type

For Open authentication mode, the selection of encryption type are NONE and WEP. For WPA-PSK, WPA2-PSK and WPA-PSK/ WPA2-PSK authentication mode, the encryption type supports TKIP, AES and TKIP/AES.

WPS Default Key Index

Shows the WEP default key (1~4).

WPS Key(ASCII)

Shows the WPS security keys (ASCII). The key can be used to ensure the security of the wireless network.

AP PIN

Here shows the AP's PIN code (Personal Identification Number) that the enrollee should enter the registrar's PIN code to make a connection.

Reset OOB

Reset WPS AP to the OOB (out-of-box) configuration.

WPS Process

WPS mode

PIN: Personal Identification Number. Select PIN then click Apply to make a WPS connection.

PBC: Push Button Communication. Select PBC then click Apply to make a WPS connection.

PIN

Personal Identification Number. Input Enrollee's Pin Code to AP-Registrar.

WPS Status

Here shows the current status of the WPS. If there is connection the status shows WSC Success, otherwise, the status shows Idle.

3.5.1.6 Station List

Here shows the station information that connected with the Wireless Portable Router.

Station List

You could monitor stations which associated to this AP here.							
Wireless Network							
MAC Address	Aid	PSM	MimoPS	MCS	BW	SGI	STBC
00:12:0E:25:47:81	1	0	3	7	40M	0	1

3.5.2 Client Mode

3.5.2.1 Station Profile

Station Profile

The Status page shows the settings and current operation status of the Station.

Profile List					
Profile	SSID	Channel	Authentication	Encryption	Network Type
<div> <input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Edit"/> <input type="button" value="Activate"/> </div>					

Click Add button to set the station profile.

System Configuration	
Profile Name	<input type="text" value="PROF001"/>
SSID	<input type="text"/>
Network Type	<input type="text" value="Infrastructure"/>
Power Saving Mode	<input checked="" type="radio"/> CAM (Constantly Awake Mode) <input type="radio"/> Power Saving Mode
RTS Threshold	<input type="checkbox"/> Used <input type="text" value="2347"/>
Fragment Threshold	<input type="checkbox"/> Used <input type="text" value="2346"/>

Security Policy	
Security Mode	<input type="text" value="OPEN"/>

Wire Equivalence Protection (WEP)	
WEP Key Length	<input type="text" value="64 bit (10 hex digits / 5 ascii keys)"/>
WEP Key Entry Method	<input type="text" value="Hexadecimal"/>
WEP Keys	WEP Key 1 : <input type="text"/>
	WEP Key 2 : <input type="text"/>
	WEP Key 3 : <input type="text"/>
	WEP Key 4 : <input type="text"/>
Default Key	<input type="text" value="Key 1"/>

Profile Name

Default profile name is PROF001, or enter desired profile name here.

SSID

Enter the station's network name here.

Network Type

Select Infrastructure or 802.11 Ad Hoc from the pull-down list.

Power Saving Mode

CAM (Constantly Awake Mode) or Power Saving Mode.

RTS Threshold

Check the box to use the function. The maximum is 2347.

Fragment

Check the box to use the function. The maximum is 2346.

Threshold

Security Mode

Select the security OPEN, SHARED, WPA-Personal or WPA2-Personal form the pull-down menu.

a) **OPEN/Shared**

Security Policy	
Security Mode	OPEN
Wire Equivalence Protection (WEP)	
WEP Key Length	64 bit (10 hex digits / 5 ascii keys)
WEP Key Entry Method	Hexadecimal
WEP Keys	WEP Key 1 :
	WEP Key 2 :
	WEP Key 3 :
	WEP Key 4 :
Default Key	Key 1
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

**WEP Key Length/
WEP Key Entry Method**

Only valid when using WEP encryption algorithm. There are several formats to enter the keys.

- Hexadecimal (64 bits) : 10 Hex characters.
- Hexadecimal (128 bits) : 26 Hex characters.
- ASCII (64 bits) : 5 ASCII characters.
- ASCII (128 bits) : 13 ASCII characters.

WEP Key 1~4

Enter the password in the encryption key field that the encryption key number must match the selected Tx key.

Default Key

There are four keys 1~4 that you can select at will. All computers, access points, and wireless adapters must use the same key when making a connection.

b) **WPA-Personal / WPA2-Personal**

Security Policy	
Security Mode	WPA-Personal
WPA	
WPA Algorithms	<input checked="" type="radio"/> TKIP <input type="radio"/> AES
Pass Phrase	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

WPA Algorithms Select TKIP or AES encryption algorithm.

Pass Phrase Enter the pass phrase 8~63 ASCII or 64 HEX characters in the column.

3.5.2.2 Station Link Status

This page shows the linking information of the station.

Station Link Status

The Status page shows the settings and current operation status of the Station.

Link Status			
Status	3GSHARE <--> 00-0C-43-30-50-30		
Extra Info	Link is Up		
Channel	6 <--> 2437000 KHz ; Central Channel: 8		
Link Speed	Tx(Mbps) 135.0	Rx(Mbps) 58.5	
Throughput	Tx(Kbps) 0.0	Rx(Kbps) 242.9	
Link Quality	Good 73%		
Signal Strength 1	Weak 32%	<input type="checkbox"/> dBm format	
Signal Strength 2	Weak 16%		
Signal Strength 3	Weak 8%		
Noise Level3	Strength 100%		

HT

BW	40
GI	long
STBC	none
MCS	7
SNR0	7
SNR1	4898576

3.5.2.3 Station Site Survey

Here shows the AP nearby, select desired AP to make a connection. Click Rescan button to survey the APs. Select preferred AP, then click Connect button to make a connection. And you can also set the preferred AP in to profile, click Add Profile to add.

Station Site Survey

Site survey page shows information of APs nearby. You may choose one of these APs connecting or adding it to profile.

Site Survey							
	SSID	BSSID	RSSI	Channel	Encryption	Authentication	Network Type
<input type="radio"/>	3089AP	00-90-CC-BE-6C-83	81%	11	Not Use	OPEN	Infrastructure
<input type="radio"/>	airlive	00-4F-62-0E-A5-4B	20%	6	Not Use	OPEN	Infrastructure
<input type="radio"/>		00-90-CC-D3-02-32	34%	6	Not Use	OPEN	Infrastructure

Connected <--> Abocom-Wireless

3.5.2.4 Station Statistics

This screen displays the transmission and reception statistics on your current networks.

Station Statistics

The Status page shows the settings and current operation status of the Station.

Transmit Statistics	
Frames Transmitted Successfully	1127
Frames Transmitted Successfully Without Retry	357
Frames Transmitted Successfully After Retry(s)	770
Frames Fail To Receive ACK After All Retries	1
RTS Frames Successfully Receive CTS	0
RTS Frames Fail To Receive CTS	0

Receive Statistics	
Frames Received Successfully	73702
Frames Received With CRC Error	62827
Frames Dropped Due To Out-of-Resource	0
Duplicate Frames Received	10

3.5.2.5 Station Advanced Configurations

Station Advanced Configurations

The Status page shows the settings and current operation status of the Station.

Advance Configuration	
Wireless Mode(Infra)	802.11 B/G/N mixed mode ▾
Country Region Code	11 B/G 0:CH1-11 ▾
B/G Protection	Auto ▾
Tx Rate	Auto ▾
<input checked="" type="checkbox"/> Tx Burst	

HT Physical Mode	
HT	<input checked="" type="radio"/> MM <input type="radio"/> GF
BW	<input type="radio"/> 20 <input checked="" type="radio"/> Auto
GI	<input type="radio"/> Long <input checked="" type="radio"/> Auto
MCS	Auto ▾

- Wireless Mode (Infra)** Select 802.11 B/G/N mixed mode, 802.11B only, 802.11G only, 802.11N only, 802.11 G/N mixed mode, or 802.11 B/G mixed mode from the pull-down menu. (Default is 802.11 B/G/N mixed mode.)
- B/G Protection** Select Auto, On or Off from the pull-down menu.
- Tx Rate** Select preferred Tx rate form the pull-down list.
- Tx Burst** Check the box to enable the Tx Burst function. (Default Tx Burst setting is Enable.)
- HT** Select MM or GF. Default setting is MM.
- BW** Channel Band Width. Select 20 or Auto. (Default setting is Auto.)
- GI** Guard Interval. Select Long or Auto. (Default setting is Auto.)
- MCS** Select form the pull-down menu 0~15, 32 or Auto. (Default setting is Auto.)
- RADIO OFF** Click this button to turn on or off the wireless function.

3.5.2.6 Station QoS

Station Advanced Configurations

The Status page shows the settings and current operation status of the Station.

Qos Configuration	
WMM	<input checked="" type="checkbox"/> enable
WMM Power Saving	<input type="checkbox"/> enable
PS Mode	<input type="checkbox"/> AC_BE <input type="checkbox"/> AC_BK <input type="checkbox"/> AC_VI <input type="checkbox"/> AC_VO
Direct Link Setup	<input type="checkbox"/> enable

Direct Link Setup	
MAC Address	<input type="text"/> - <input type="text"/> - <input type="text"/> - <input type="text"/> - <input type="text"/> - <input type="text"/>
Timeout Value	sec

DLS Status	
MAC Address	Timeout

- WMM** Check the box to enable or disable the WMM function. (Default setting is Enable.)
- WMM Power Saving** Check the box to enable this function. (Default setting is Disable.)
- PS Mode** Select preferred power save mode, AC_BE, AC_BK, AC_VI, AC_VO.

- Direct Link Setup

Check the box to enable Direct Link Setup (DLS) and enter the MAC address in below column. This function will be enabled under the connection with AP which must support the DLS function. Direct Link Setup allows direct STA-to-STA frame transfer within a BSS (Basic Service Set). This is designed for consumer use, where STA-to-STA transfer is more commonly used.
- Tear Down

Click the Tear Down button to disable the DLS function.

3.5.2.7 Station 11n Configurations

Station 11n Configurations

The Status page shows the settings and current operation status of the Station.

11n Configuration

MPDU Aggregation	<input type="checkbox"/> enable
<input checked="" type="radio"/> Manual <input type="radio"/> Auto	
MPDU density	0
Aggregation MSDU(A-MSDU)	<input type="checkbox"/> enable

Apply

- MPDU Aggregation

Check the box to enable this function. (Default setting is Disable.) Select Manual or Auto to set up the MPDU density form 0~7. Default setting is Auto.
- Aggregation MSDU (A-MSDU)

Check the box to enable this function. (Default setting is Disable.)

3.5.2.8 Station About

Here shows the information of the station.

Station About

The Status page shows the settings and current operation status of the Station.

About

Driver Version	1.8.0.0
MAC Address	00-0C-43-30-50-88

3.5.2.9 Wi-Fi Protected Setup (STA)

This page allows you to use the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client atomically synchronizes its setting and connect to the Access Point in a minute without any hassle.

Wi-Fi Protected Setup (STA)

You could setup security easily by choosing PIN or PBC method to do Wi-Fi Protected Setup.

WPS AP site survey								
No.	SSID	BSSID	RSSI	Ch.	Auth.	Encrypt	Ver.	Status
<input checked="" type="radio"/>	ZyXEL-NBG-417N	00BB97530334	44%	1	OPEN	Not Use	1.0	Conf.
<input type="radio"/>	55	000000114904	76%	6	Unknown	WEP	1.0	Conf.
<input type="radio"/>	ZyXEL	0019CBD5F09C	50%	6	OPEN	Not Use	1.0	Unconf.
<input type="radio"/>	WR5502-FAE	00E04C865101	24%	6	OPEN	Not Use	1.0	Conf.
<input type="radio"/>	skl	0090CCF3893C	0%	10	OPEN	Not Use	1.0	Conf.
<input type="radio"/>	3059	00E098286011	60%	11	Unknown	WEP	1.0	Conf.
<input type="radio"/>	3090_ZyXEL	000C43418844	5%	6	Unknown	WEP	1.0	Conf.

UUID: 2880288028801880a88000bb97530334
RF Band: 2.4G/5G

Refresh Mode: Enrollee PIN: 31663441

PIN Start PBC Start Cancel

Renew PIN

WPS Status

Not used

WPS AP Site Survey

Display the information of surrounding APs with WPS function from last scan result. List information included SSID, BSSID, RSSI, Channel, Authentication, Encryption, Version, and Status.

Refresh

Issue a rescan command to wireless NIC to update information on surrounding wireless network.

Mode

Select from the pull-down menu to decide the station role-playing as an Enrollee or an external Registrar.

Registrar: Add the AP's PIN code into the PIN code column, and press the device PIN button. It will connect with the AP in 2 minutes and get IP address.

Enrollee: Input the device's PIN code into the PIN code column of AP. Start AP WPS process and click device PIN button. Then, the device will connect to AP in two minutes and get IP address.

PIN Start

It is required to enter PIN (Personal Identification Number) Code (8-digit numbers) into Registrar when using PIN method. When STA is Enrollee, users can use "Renew PIN" button to re-generate new PIN Code.

PBC Start

Push Button Communication. Click Start PBC button to make a WPS connection within 2 minutes.

Cancel

Click Cancel button to discard the WPS connection.

WPS Status

Here shows the current status of the WPS function.

3.6 Firewall

3.6.1 MAC/IP/Port Filtering

MAC/IP/Port Filtering Settings

You may setup firewall rules to protect your network from virus, worm and malicious activity on the Internet.

Basic Settings

MAC/IP/Port Filtering Enable

Default Policy -- The packet that don't match with any rules would be: Dropped

Apply Reset

MAC/IP/Port Filter Settings

MAC address

Dest IP Address

Source IP Address

Protocol None

Dest Port Range -

Source Port Range -

Action Accept

Comment

(The maximum rule count is 32.)

Apply Reset

Current MAC/IP/Port filtering rules in system:

No.	MAC address	Dest IP Address	Source IP Address	Protocol	Dest Port Range	Source Port Range	Action	Comment	Pkt Cnt
1	<input type="checkbox"/> 00:12:0E:25:47:81	10.10.10.101	255.255.255.0	-	-	-	Accept		0
Others would be dropped									-

Delete Selected Reset

MAC/IP/Port Filtering

Default Policy

Select Enable or Disable from the pull-down list.

Select Accepted or Dropped from the pull-down menu, to accept or deny connection for the MAC that user set in below settings.

Apply

Click to save and apply the current settings.

Reset

Press to discard the current settings.

MAC Address

Enter the client MAC address that user would like to connect(accept) or disconnect(drop).

Dest IP Address

Enter the local server's IP address.

Source IP Address

Enter the source IP address.

Protocol

Select the protocol (None, TCP, UDP or ICMP) used to the remote system or service.

Dest Port Range

For TCP and UDP services enter the beginning of the range of port numbers used by the service. If the service uses a single port number, enter it in both the start and finish fields.

Source Port Range

Action

Select rules for DROP, or rules for ACCEPT form the pull-down menu. Select Drop to disconnect with the Wireless Portable Router that MAC address has be set, and ACCEPT to allow the device that connect with the Wireless Portable Router.

Comment

Key in a description for these settings.

3.6.2 Port Forwarding

Virtual Server Settings

You may setup Virtual Servers to provide services on Internet.

Virtual Server Settings	
Virtual Server Settings	Disable ▾
IP Address	<input type="text"/>
Port Range	<input type="text"/> <input type="text"/>
Protocol	TCP&UDP ▾
Comment	<input type="text"/>

(The maximum rule count is 32.)

Current Virtual Servers in system:

No.	IP Address	Port Range	Protocol	Comment
<input type="button" value="Delete Selected"/> <input type="button" value="Reset"/>				

Virtual Server Settings Select Enable or Disable from the pull-down menu.

IP Address Enter the local server's IP address.

Port Range For TCP and UDP services enter the beginning of the range of port numbers used by the service. If the service uses a single port number, enter it in both the start and finish fields.

Protocol Select the protocol (TCP, UDP or TCP&UDP) used to the remote system or service.

Comment You may key in a description for the IP address.

3.6.3 DMZ

DMZ Settings

You may setup a De-militarized Zone(DMZ) to separate Internal network and Internet.

DMZ Settings	
DMZ Settings	Disable ▾
DMZ IP Address	<input type="text"/>

DMZ Settings If the DMZ Host Function is enabled, it means that you set up DMZ host at a particular computer to be exposed to the Internet so that some applications/software, especially Internet / online game can have two-way connections. Select Enable or Disable from the pull-down menu.

DMZ IP Address Enter the IP address of a particular host in your LAN that will receive all the packets originally going to the WAN port/ Public IP address above.
Note: You need to give your LAN PC clients a fixed/ static IP address for DMZ to work properly.

Apply Click to save and apply the current settings.

Reset Press to discard current settings.

3.6.4 System Security

System Security Settings

You may configure the system firewall to protect AP/Router itself from attacking.

Remote management

Remote management (via WAN)Deny

Ping form WAN Filter

Ping form WAN FilterDisable

Stateful Packet Inspection (SPI)

SPI FirewallDisable

Apply

Reset

- Remote management**

Remote management (via WAN)

Select Deny or Allow form the pull-down list to enable or disable the remote client to control the Wireless Portable Router via WAN. Default setting is Deny.
- Ping form WAN Filter**

Ping form WAN Filter

Select Disable or Enable from the pull-down list. Default setting is Disable.
- Stateful Packet Inspection (SPI)**

SPI Firewall

Stateful packet inspection (SPI) is a firewall that keeps track of the state of network connections (such as TCP streams, UDP communication) traveling across it. The firewall is programmed to distinguish legitimate packets for different types of connections. Only packets matching a known connection state will be allowed by the firewall; others will be rejected.

Select Disable or Enable the SPI firewall function from the pull-down list. Default setting is Disable.

3.6.5 Content Filtering

Content Filter Settings

You can setup Content Filter to restrict the improper content access.

Webs Content Filter

Filters: ☐ Proxy ☐ Java ☐ ActiveX

Apply

Reset

Webs URL Filter Settings

Current Webs URL Filters:

No URL

Delete

Reset

Add a URL filter:

URL:

Add

Reset

Webs Host Filter Settings

Current Website Host Filters:

No Host(keyword)

Delete

Reset

Add a Host(keyword) Filter:

Keyword

Add

Reset

Webs Content Filter Settings

Select Webs Content Filters, Proxy, Java or ActiveX.

Webs URL Filter Settings

Enter the IP address for URL filtering.

Webs Host Filter Settings

Enter the keyword in the field for a host filtering.

3.7 Administrators

3.7.1 Management

System Management

You may configure administrator account and password, NTP settings, and Dynamic DNS settings here.

Administrator Settings

Account:

Password:

NTP Settings

Current Time:

Time Zone:

NTP Server:
ntp0.broad.mit.edu
time.stdtime.gov.tw

NTP synchronization(hours):

Green AP:

Duration	Action
<input type="text" value="00"/> : <input type="text" value="00"/> ~ <input type="text" value="00"/> : <input type="text" value="00"/>	<input type="text" value="Disable"/>
<input type="text" value="00"/> : <input type="text" value="00"/> ~ <input type="text" value="00"/> : <input type="text" value="00"/>	<input type="text" value="Disable"/>
<input type="text" value="00"/> : <input type="text" value="00"/> ~ <input type="text" value="00"/> : <input type="text" value="00"/>	<input type="text" value="Disable"/>
<input type="text" value="00"/> : <input type="text" value="00"/> ~ <input type="text" value="00"/> : <input type="text" value="00"/>	<input type="text" value="Disable"/>

DDNS Settings

Dynamic DNS Provider:

Account:

Password:

DDNS:

Result:

Administrator Settings

Account

Key in a new login user name in the blank field.

Password

Maximum input is 36 alphanumeric characters (case sensitive.)

NTP Settings

Current Time

Click Sync with host button to synchronize the time with the server.

Time Zone

Select the time zone area that you located from the pull-down list.

NTP Server

Enter the Network Time Protocol Server here. Ex: time.nist.gov, ntp0.broad.mit.edu, or time.stdtime.gov.tw.

NTP synchronization(hours)

Enter the hour(s) here to synchronize time of the Wireless Portable Router with the server selected.

Green AP

Duration	User has to set up the NTP Server and NTP synchronization(hours) first that the Green AP function can be set up. Set up a period of time to enable or disable the wireless TX function.
Action	Select Disable, WiFi TX power OFF, WiFi TX power 25%, WiFi TX power 50%, or WiFi TX power 75% from the pull-down menu, to enable or disable the wireless TX function of the Wireless Portable Router.

DDNS Settings

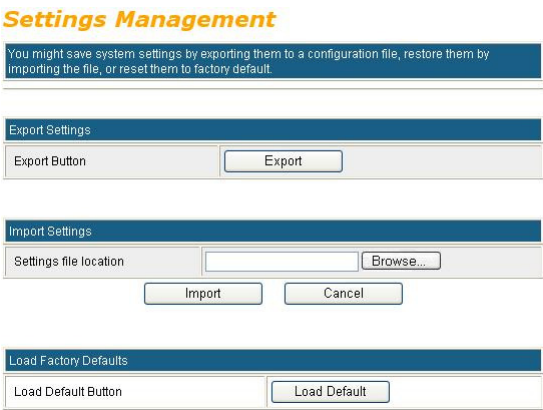
Dynamic DNS Provider	Select the DNS provider form the pull-down list. DNS provider is a company that provides access to the internet.
Account	Enter your account that you registered in DNS provider website.
Password	Enter your passwords that you registered.
DDNS	Apply for a Domain Name, and ensure it is allocated to you.
Result	Here shows the DDNS status.

3.7.2 Upload Firmware



Location	Click the Browse... button, find and open the firmware file (the browser will display to correct file path) then click Apply to upgrade the Wireless Portable Router's firmware.
----------	--

3.7.3 Settings Management



Export Settings

Export Button

Click the Export button to save the current device settings to located computer.

Import Settings

Import

Click the Browse... button, find and open the settings file (the browser will display to correct file path), then click the Import button to use the device settings that previous saved.

Cancel

Click to discard the file that you selected form your located computer.

Load Factory Defaults

Load Default Button

Click to Load Default button to set the Wireless Portable Router back to factory default settings.

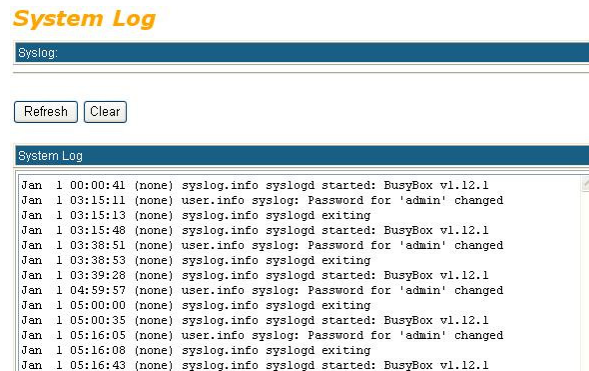
3.7.4 Statistics

This page shows all system memory, WAN/LAN, all interfaces statistics.

Statistic	
Take a look at the Ralink SoC statistics	
Memory	
Memory total:	13584 kB
Memory left:	3356 kB
WAN/LAN	
WAN Rx packets:	0
WAN Rx bytes:	0
WAN Tx packets:	3224
WAN Tx bytes:	1908912
LAN Rx packets:	250
LAN Rx bytes:	27790
LAN Tx packets:	324
LAN Tx bytes:	158517

3.7.5 System Log

Here shows the system log file information. Click Refresh button to update system log file, or click Clear button to review the log file.



3.7.6 System Reboot

Click the Reboot button to restart the Wireless Portable Router.



Chapter 4: PC Configuration

4.1 Overview

For each PC, the following may need to be configured:

- TCP/IP network settings
- Internet Access configuration
- Wireless configuration

4.2 Windows Clients

- This section describes how to configure Windows clients for Internet access via the Wireless Portable Router.
- The first step is to check the PC's TCP/IP settings.
- The Wireless Portable Router uses the TCP/IP network protocol for all functions, so it is essential that the TCP/IP protocol be installed and configured on each PC.

4.2.1 TCP/IP Settings - Overview

If using default Wireless Portable Router settings, and default Windows TCP/IP settings, no changes need to be made.

- By default, the Wireless Portable Router will act as a DHCP Server, automatically providing a suitable IP Address (and related information) to each PC when the PC boots.
- For all non-Server versions of Windows, the default TCP/IP setting is to act as a DHCP client.

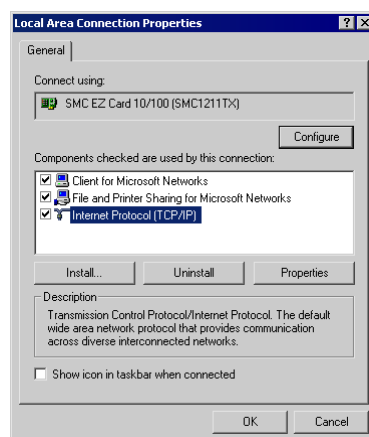
If using a Fixed (specified) IP address, the following changes are required:

- The Gateway must be set to the IP address of the Wireless Portable Router.
- The DNS should be set to the address provided by your ISP.

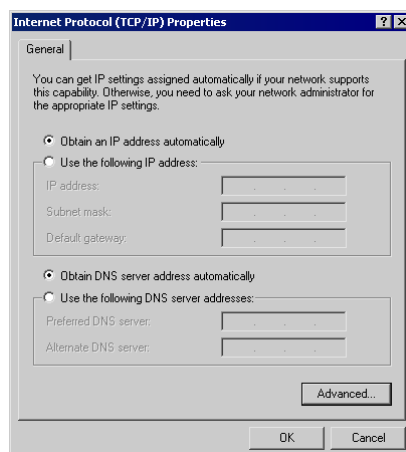
4.2.2 Checking TCP/IP Settings - Windows 2000

1. Select Control Panel - Network and Dial-up Connection.

2. Right - click the Local Area Connection icon and select Properties. You should see a screen like the following:



3. Select the TCP/IP protocol for your network card.
4. Click on the Properties button. You should then see a screen like the following.



5. Ensure your TCP/IP settings are correct, as described below.

4.2.2.1 Using DHCP

- To use DHCP, select the radio button Obtain an IP Address automatically. This is the default Windows setting. Using this is recommended. By default, the Wireless Portable Router will act as a DHCP Server.
- Restart your PC to ensure it obtains an IP Address from the Wireless Portable Router.

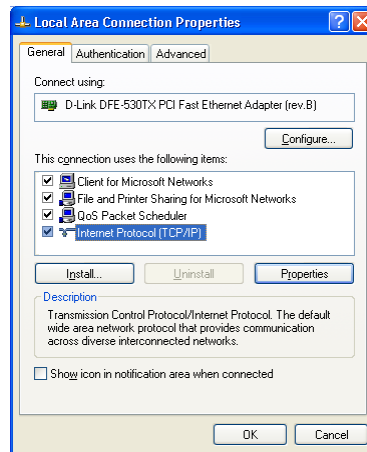
4.2.2.2 Using a fixed IP Address ("Use the following IP Address")

If your PC is already configured, check with your network administrator before making the following changes.

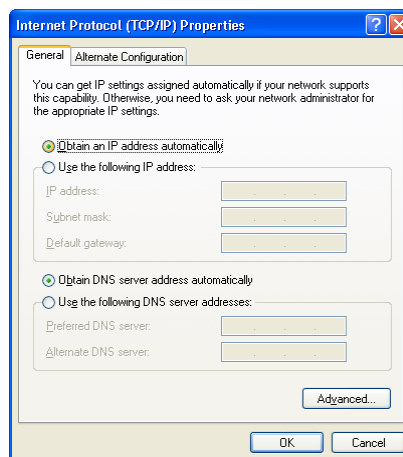
- Enter the Wireless Portable Router 's IP address in the Default gateway field and click OK. (Your LAN administrator can advise you of the IP Address they assigned to the Wireless Portable Router.)
- If the DNS Server fields are empty, select Use the following DNS server addresses, and enters the DNS address or addresses provided by your ISP, then click OK.

4.2.3 Checking TCP/IP Settings - Windows XP

1. Select Control Panel - Network Connection.
2. Right click the Local Area Connection and choose Properties. You should see a screen like the following:



3. Select the TCP/IP protocol for your network card.
4. Click on the Properties button. You should then see a screen like the following.



5. Ensure your TCP/IP settings are correct.

4.2.3.1 Using DHCP

- To use DHCP, select the radio button Obtain an IP Address automatically. This is the default Windows setting. Using this is recommended. By default, the Wireless Portable Router will act as a DHCP Server.
- Restart your PC to ensure it obtains an IP Address from the Wireless Portable Router.
- Using a fixed IP Address ("Use the following IP Address")
- If your PC is already configured, check with your network administrator before making the following changes.
- In the Default gateway field, enter the Wireless Portable Router 's IP address and click OK. Your LAN administrator can advise you of the IP Address they assigned to the Wireless Portable Router.

- If the DNS Server fields are empty, select Use the following DNS server addresses, and enters the DNS address or addresses provided by your ISP, then click OK.

4.2.4 Internet Access

To configure your PCs to use the Wireless Portable Router for Internet access:

- Ensure that the ADSL modem, DSL modem, Cable modem, or other permanent connection is functional.
- Use the following procedure to configure your Browser to access the Internet via the LAN, rather than by a Dial-up connection.

4.2.4.1 For Windows 2000

1. Select Start Menu - Settings - Control Panel - Internet Options.
2. Select the Connection tab, and click the Setup button.
3. Select "I want to set up my Internet connection manually, or I want to connect through a local area network (LAN)" and click Next.
4. Select "I connect through a local area network (LAN)" and click Next.
5. Ensure all of the boxes on the following Local area network Internet Configuration screen are unchecked.
6. Check the "No" option when prompted "Do you want to set up an Internet mail account now?"
7. Click Finish to close the Internet Connection Wizard. Setup is now completed.

4.2.4.2 For Windows XP

1. Select Start Menu - Control Panel - Network and Internet Connections.
2. Select Set up or change your Internet Connection.
3. Select the Connection tab, and click the Setup button.
4. Cancel the pop-up "Location Information" screen.
5. Click Next on the "New Connection Wizard" screen.
6. Select "Connect to the Internet" and click Next.
7. Select "Set up my connection manually" and click Next.
8. Check "Connect using a broadband connection that is always on" and click Next.
9. Click Finish to close the New Connection Wizard. Setup is now completed.

4.2.4.3 Accessing AOL

To access AOL (America On Line) through the Wireless Portable Router, the AOL for Windows software must be configured to use TCP/IP network access, rather than a dial-up connection. The configuration process is as follows:

1. Start the AOL for Windows communication software. Ensure that it is Version 2.5, 3.0 or later. This procedure will not work with earlier versions.
2. Click the Setup button.
3. Select Create Location, and change the location name from "New Locality" to " Wireless Portable Router ".
4. Click Edit Location. Select TCP/IP for the Network field. (Leave the Phone Number blank.)
5. Click Save, then OK.
6. Configuration is now complete.
7. Before clicking "Sign On", always ensure that you are using the " Wireless Portable Router " location.

4.3 Macintosh Clients

From your Macintosh, you can access the Internet via the Wireless Portable Router. The procedure is as follows.

1. Open the TCP/IP Control Panel.
2. Select Ethernet from the Connect via pop-up menu.
3. Select Using DHCP Server from the Configure pop-up menu. The DHCP Client ID field can be left blank.
4. Close the TCP/IP panel, saving your settings.

Note:

If using manually assigned IP addresses instead of DHCP, the required changes are:

- Set the Router Address field to the Wireless Portable Router 's IP Address.
- Ensure your DNS settings are correct.

4.4 Linux Clients

To access the Internet via the Wireless Portable Router, it is only necessary to set the Wireless Portable Router as the "Gateway".

Ensure you are logged in as "root" before attempting any changes.

4.4.1 Fixed IP Address

By default, most Unix installations use a fixed IP Address. If you wish to continue using a fixed IP Address, make the following changes to your configuration.

- Set your "Default Gateway" to the IP Address of the Wireless Portable Router.
- Ensure your DNS (Domain Name server) settings are correct.

4.4.2 To act as a DHCP Client (Recommended)

The procedure below may vary according to your version of Linux and X -windows shell.

1. Start your X Windows client.
2. Select Control Panel – Network.
3. Select the "Interface" entry for your Network card. Normally, this will be called "eth0".
4. Click the Edit button, set the "protocol" to "DHCP", and save this data.
5. To apply your changes:
 - Use the "Deactivate" and "Activate" buttons, if available.
 - OR, restart your system.

4.5 Other Unix Systems

To access the Internet via the Wireless Portable Router:

- Ensure the "Gateway" field for your network card is set to the IP Address of the Wireless Portable Router.
- Ensure your DNS (Name Server) settings are correct.

4.6 Wireless Station Configuration

- This section applies to all wireless stations wishing to use the Wireless Portable Router 's access point, regardless of the operating system that is used on the client.
- To use the Wireless Portable Router, each wireless station must have compatible settings, as following:

Mode	The mode must be set to Infrastructure.
SSID (ESSID)	The network name must match the value used on the Wireless Portable Router. Note! The SSID is case sensitive.
Open Shared Key	If there is no security is enabled on the Wireless Portable Router, the security of each station should be disabled as well. And, you can connect the Wireless Portable Router without security, but it is NOT recommended.
WEP auto	By default, WEP on the Wireless Portable Router is disabled. If WEP remains disabled on the Wireless Portable Router, all stations must have WEP disabled. If WEP is enabled on the Wireless Portable Router, each station must use the same settings as the Wireless Portable Router.
WPA-PSK WPA2-PSK WPA-PSK WPA2-PSK	WPA-PSK (TKIP/AES)/ WPA2-PSK (TKIP/AES)/ WPA-RADIUS (TKIP/AES)/ WPA2 - RADIUS (TKIP/AES): If one of these securities is enabled on the Wireless Portable Router. To make a connection, each station must use the same algorithms and pass phrase as the Wireless Portable Router.
WPA WPA2 WPA WPA2 802.1x	RADIUS Server: RADIUS is an authentication, authorization and accounting client-server protocol. The client is a Network Access Server that desires to authenticate its links. The server is a server that has access to a user database with authentication information. Each station must set up the RADIUS Server's IP address, port and passwords that provided by your ISP.

Note:

By default, the Wireless Portable Router will allow 802.11b, 802.11g and 802.11n connections.

Appendix A: Troubleshooting

A.1 Overview

This chapter covers some common problems that may be encountered while using the Wireless Portable Router and some possible solutions to them. If you follow the suggested steps and the Wireless Portable Router still does not function properly, contact your dealer for further advice.

A.2 General Problems

Problem 1: Can't connect to the Wireless Portable Router to configure it.

Solution 1: Check the following:

1. Check the Wireless Portable Router is properly installed, LAN connections are OK, and it is powered ON.
2. Ensure that your PC and the Wireless Portable Router are on the same network segment.
3. If your PC is set to "Obtain an IP Address automatically" (DHCP client), please restart it.
4. If your PC uses a Fixed (Static) IP address, ensure that it is using an IP Address within the range 192.168.10.1 to 192.168.10.253 and thus compatible with the Wireless Portable Router's default IP Address of 192.168.10.254.

Also, the Network Mask should be set to 255.255.255.0 to match the Wireless Portable Router.

In Windows, you can check these settings by using Control Panel-Network to check the Properties for the TCP/IP protocol.

A.3 Internet Access

Problem 1: When I enter a URL or IP address I get a time out error.

Solution 1: A number of things could be causing this. Try the following troubleshooting steps.

- Check if other PCs work. If they do, ensure that your PCs IP settings are correct. If using a Fixed (Static) IP Address, check the Network Mask, Default gateway and DNS as well as the IP Address.
- If the PCs are configured correctly, but still not working, check the Wireless Portable Router. Ensure that it is connected and ON. Connect to it and check its settings. (If you can't connect to it, check the LAN and power connections.)
- If the Wireless Portable Router is configured correctly, check your Internet connection (DSL/Cable modem etc) to see that it is working correctly.

Problem 2: Some applications do not run properly when using the Wireless Portable Router.

Solution 2: The Wireless Portable Router processes the data passing through it, so it is not transparent.

Use the Content Filter Settings feature to allow the use of Internet applications, which do not function correctly.

If this does solve the problem you can use the DMZ function. This should work with almost every application, but:

- It is a security risk, since the firewall is disabled.
- Only one (1) PC can use this feature.

A.4 Wireless Access

Problem 1: My PC can't locate the Wireless Portable Router.

Solution 1: Check the following:

1. Your PC is set to Infrastructure Mode. (Access Points are always in Infrastructure Mode)
2. The SSID on your PC and the Wireless Portable Router are the same.
Remember that the SSID is case-sensitive. So, for example "Workgroup" does NOT match "workgroup."
3. Both your PC and the Wireless Portable Router must have the same setting for security.
The default setting for the Wireless Portable Router security is disabled, so your wireless station should also have security disabled.
4. If security is enabled on the Wireless Portable Router, your PC must have security enabled, and the key must be matched.
5. To see if radio interference is causing a problem, see if connection is possible when close to the Wireless Portable Router.
Remember that the connection range can be as little as 100 feet in poor environments.

Problem 2: Wireless connection speed is very slow.

Solution 2: The wireless system will connect at the highest possible speed, depending on the distance and the environment. To obtain the highest possible connection speed, you can experiment with the following:

1. Wireless Portable Router location
Try adjusting the location and orientation of the Wireless Portable Router.
2. Wireless Channel
If interference is the problem, changing to another channel may show a marked improvement.
3. Radio Interference
Other devices may be causing interference. You can experiment by switching other devices off, and see if this helps. Any "noisy" devices should be shielded or relocated.
4. RF Shielding
Your environment may tend to block transmission between the wireless stations. This will mean high access speed is only possible when close to the Wireless Portable Router.

Appendix B: About Wireless LANs

B.1 BBS

A group of Wireless Stations and a single Access Point, all using the same ID (SSID), form a Basic Service Set (BSS).

Using the same SSID is essential. Devices with different SSIDs are unable to communicate with each other.

B.2 Channels

The Wireless Channel sets the radio frequency used for communication.

- Access Points use a fixed Channel. You can select the Channel used. This allows you to choose a Channel which provides the least interference and best performance. In the USA and Canada, 11 channels are available. If using multiple Access Points, it is better if adjacent Access Points use different Channels to reduce interference.
- In "Infrastructure" mode, Wireless Stations normally scan all Channels, looking for an Access Point. If more than one Access Point can be used, the one with the strongest signal is used. (This can only happen within an ESS.)

Note to US model owner: To comply with US FCC regulation, the country selection function has been completely removed from all US models. The above function is for non-US models only.

B.3 Security

B3.1 WEP

WEP (Wired Equivalent Privacy) is a standard for encrypting data before it is transmitted. This is desirable because it is impossible to prevent snoopers from receiving any data which is transmitted

by your Wireless Stations. But if the data is encrypted, then it is meaningless unless the receiver can decrypt it.

If WEP is used, the Wireless Stations and the Access Point must have the same security settings for each of the following:

WEP	64 Bits, 128 Bits.
Key	For 64 Bits encryption, the Key value must match. For 128 Bits encryption, the Key value must match.
WEP Authentication	Open System or Shared Key.

B3.2 WPA/WPA2

WPA/WPA2 (Wi-Fi Protected Access) is more secure than WEP. It uses a "Shared Key" which allows the encryption keys to be regenerated at a specified interval. There are several encryption options: TKIP, AES, TKIP-AES and additional setup for RADIUS is required in this method. The most important features beyond WPA to become standardized through 802.11i/WPA2 are: pre-authentication, which enables secure fast roaming without noticeable signal latency.

If WPA or WPA2 is used, the Wireless Stations and the Access Point must have the same security settings.

B3.3 WPA-PSK/WPA2-PSK

WPA/WPA2 (Wi-Fi Protected Access using Pre-Shared Key) is recommended for users who are not using a RADIUS server in a home environment and all their clients support WPA/WPA2. This method provides a better security.

If WPA-PSK or WPA2-PSK is used, the Wireless Stations and the Access Point must have the same security settings.

Encryption	WEP Key 1~4	Passphrase
TKIP	NOT REQUIRED	8-63 characters
Encryption		

B3.4 802.1x

With 802.1x authentication, a wireless PC can join any network and receive any messages that are not encrypted, however, additional setup for RADIUS to issue the WEP key dynamically will be required.

RADIUS is an authentication, authorization, and accounting client-server protocol. The client is a Network Access Server that desires to authenticate its links. The server is a server that has access to a user database with authentication information.

B.4 Wireless LAN Configuration

To allow Wireless Stations to use the Access Point, the Wireless Stations and the Access Point must use the same settings, as follows:

Mode	The mode must be set to Infrastructure.
SSID (ESSID)	The network name must match the value used on the Wireless Portable Router. Note! The SSID is case sensitive.
Open Shared Key	If there is no security is enabled on the Wireless Portable Router, the security of each station should be disabled as well. And, you can connect the Wireless Portable Router without security, but it is NOT recommended.
WEP AUTO	By default, WEP on the Wireless Portable Router is disabled. If WEP remains disabled on the Wireless Portable Router, all stations must have WEP disabled. If WEP is enabled on the Wireless Portable Router, each station must use the same settings as the Wireless Portable Router.
WPA-PSK WPA2-PSK WPA-PSK WPA2-PSK	WPA-PSK (TKIP/AES)/ WPA2-PSK (TKIP/AES): If one of these securities is enabled on the Wireless Portable Router. To make a connection, each station must use the same algorithms and pass phrase as the Wireless Portable Router.
WPA WPA2 WPA WPA2 802.1x	RADIUS Server: RADIUS is an authentication, authorization and accounting client-server protocol. The client is a Network Access Server that desires to authenticate its links. The server is a server that has access to a user database with authentication information. Each station must set up the RADIUS Server's IP address, port and passwords that provided by your ISP.

Appendix C: Technical Support

C.1 Register Online for Free Warranty

C.1.1 Free Technical Support Hotline:

Monday to Friday, 9.00 am – 6.00 pm (Closed on Saturday, Sunday and Public Holidays)

- Singapore : (65) 6357 0668
- Malaysia : (60) 3 8023 9151
- Indonesia : (62) 21 628 3205

C.1.2 Walk-In

Monday to Friday, 9.00 am – 6.00 pm (Closed on Saturday, Sunday and Public Holidays)

- Singapore : FIDA INTERNATIONAL (S) PTE LTD
Block 16 Kallang Place, #06-02 Kallang Basin Industrial Estate, Singapore 339156.
- Malaysia : FIDA SYSTEMS (M) SDN BHD
29 Jalan USJ 1/31, 47600 Subang Jaya, Selangor Darul Ehsan, Malaysia.
- Indonesia : PROLiNK INDONESIA
P. Jayakarta Komplek 85 BR/AJ, Jakarta Pusat - Indonesia.

C.1.3 Online Technical Supports

- Singapore : support@fida.com
- Malaysia : support_my@fida.com
- Indonesia : support@prolink.co.id

This Page is Leave Blank!

Register Online For Your Product Warranty
www.prolink2u.com

SINGAPORE	FIDA INTERNATIONAL (S) PTE LTD Address : Block 16 Kallang Place, #06-02 Kallang Basin Industrial Estate, Singapore 339156. Tel : (65) 6357 0668 Email : support@fida.com
MALAYSIA	FIDA SYSTEMS (M) SDN BHD Address : 29 Jalan USJ 1/31, 47600 Subang Jaya, Selangor Darul Ehsan, Malaysia. Tel : (60) 3 8024 9151 Email : support_my@fida.com
INDONESIA	PROLiNK INDONESIA Address : P. Jayakarta Komplek 85 BR/AJ, Jakarta Pusat - Indonesia. Tel : (62) 21 628 3205 Email : support@prolink.co.id